REMARKS

Applicant appreciates the Examiner's attention to this Application.

The Office Action rejects all of the claims under 35 U.S.C. 103(a) as unpatentable over "TKEY Secret Key Renewal Mode," by Yuji Kamite, dated May 11, 2002, from http://tools.ietf.org/html/draft-ietf-dnsext-tkey-renewal-mode-01 ("IETF").

This response cancels all of the original claims and enters new claims 26-49, of which claims 26, 36, and 44 are independent. The new independent claims clarify certain features of at least one embodiment of the present invention. For instance, claim 26 recites that a new content protection implementation is automatically pushed to a device on a periodic basis, and the new content protection implementation comprises "(a) new software to replace at least part of the existing software for presenting protected content and (b) a new key to supersede the existing key for facilitating presentation of protected content." In addition, claim 26 recites that revocation data to identify a revoked key "is pushed to the device after a corresponding new content protection implementation has already been pushed to the device to equip the device with a replacement key for the revoked key." Moreover, claim 26 recites that the new content protection implementation is pushed to the device "based on a predetermined time period, without regard to whether or not the existing key has been compromised."

The Office Action refers to Sections 2.1 and 2.3 of IETF. IETF discusses the TSIG (transaction signature) computer networking protocol. As explained by wikipedia at http://en.wikipedia.org/wiki/TSIG, the TSIG protocol is defined in RFC 2845, and it is used "primarily by the Domain Name System (DNS) to provide a means of authenticating updates to a Dynamic DNS database. TSIG uses shared secret keys and one-way hashing to provide a cryptographically secure means of identifying each endpoint of a connection as being allowed to make or respond to a DNS update.... A timestamp is included in the TSIG protocol to prevent recorded responses from being reused."

The heading of Section 2.1 of IETF is "Key Usage Time Check," and the body of Section 2.1 indicates that a server can store the following information about keys to be used by clients: inception time, partial revocation time, and expiry limit. When the server receives a signed query, the server finds the key that was used for signing the query, and the server checks the inception time, partial revocation time, and expiry limit for that key, to determine whether they key is valid, partially expired, or completely expired. If the key is partially expired, the server sends the client an error message indicating that the key is partially expired.

Section 2.3 explains that the client may request a new key, in response to that error message. ("If a client has received a PartialRevoke Error ..., it sends a TKEY query ... for key renewal to the server.") The server may then create a new key with new time attributes (i.e., the inception time, partial revocation time, and expiry limit). For instance, the server can determine the "Expiry Limit," set "Inception" to "the time when the new key is actually generated," and set the "Partial Revocation Time" to "any value as long as it is between Inception and Expiry Limit." The server may then send the new key to the client.

Thus, IETF describes a server that keeps a database of expiration times for keys, and sends error messages when clients use expired keys, as well as a corresponding client that can request a new key in response to such an error message. Thus, clients can "pull" a new key from the server in response to getting an error when trying to use an existing key.

By contrast, claim 26 of the present application indicates that new keys are pushed to clients before old keys are revoked. For instance, as indicated above, claim 26 recites that "the revocation data to identify a revoked key is pushed to the device after a corresponding new content protection implementation has already been pushed to the device to equip the device with a replacement key for the revoked key." The cited portions of IETF do not disclose or suggest this feature. For at least the foregoing reasons, the Office Action does not make out a prima facie case of obviousness for claim 26.

Independent claims 36 and 44 also pertain to a new content protection implementation that is automatically pushed to a device on a periodic basis, wherein the new content protection implementation comprise (a) new software to replace at least part of the existing software for presenting protected content and (b) a new key to supersede the existing key for facilitating presentation of protected content. Claim 36 also indicates that revocation data to identify a revoked key "is pushed to the device after a corresponding new content protection implementation has already been pushed to the device to equip the device with a replacement key for the revoked key." Also, claim 44 indicates that the device receives the new content protection implementation "based on a predetermined time period, without regard to whether or not the existing key has been compromised." IETF does not discloses or suggest these features. For at least the foregoing reasons, the Office Action does not establish a prima facie vase of obviousness for any of the independent claims.

In addition, the dependent claims implicitly include the features of the respective parent claims. For at least the foregoing reasons, the Office Action does not make out a prima facie case of obviousness for any of the pending claims. The rejections should therefore be withdrawn.

CONCLUSION

For all of the foregoing reasons, reconsideration of the present application is respectfully requested.

If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927.

Respectfully submitted,

Dated: Jan. 15, 2007

/ Michael R. Barre /
Michael R. Barré
Registration No. 44,023
Patent Attorney
Intel Americas, Inc.
(512) 732-3927

Intel Corporation
c/o Intellevate, LLC
P.O. Box 52050
Minneapolis, MN 55402